arXiv:0906.2547v2 [quant-ph] 29 Sep 2009

Superactivation of the Asymptotic Zero-Error Classical Capacity of a Quantum Channel

Toby S. Cubitt*[1], Jianxin Chen†[2], and Aram W. Harrow‡[1]

[1] *Department of Mathematics, University of Bristol*
University Walk, Bristol BS8 1TW, United Kingdom
[2] *State Key Laboratory of Intelligent Technology and Systems*
Department of Computer Science and Technology, Tsinghua University
Beijing 100084, China

September 29, 2009

Abstract

The zero-error classical capacity of a quantum channel is the asymptotic rate at which it can be used to send classical bits perfectly, so that they can be decoded with zero probability of error. We show that there exist pairs of quantum channels, neither of which individually have any zero-error capacity whatsoever (even if arbitrarily many uses of the channels are available), but such that access to even a single copy of both channels allows classical information to be sent perfectly reliably. In other words, we prove that the zero-error classical capacity can be superactivated. This result is the first example of superactivation of a *classical* capacity of a quantum channel.

1 Introduction

Shannon's information theory has been highly successful at describing classical information transmission, but only in the last couple of decades or so has there been a major effort to extend it to quantum channels, and even quantum information, that we must contend with in the real world. A major strength of Shannon's work is that the calculation of asymptotic capacities, although potentially requiring optimisations over unbounded numbers of channel uses, typically reduces to a simple, and often convex, optimisation problem over a single use of a channel (a *single-letter formula*). Moreover, many of these capacities are *additive*, meaning that access to two channels together allows one to send information at a rate equal to the sum of the channels' individual capacities. These two properties—additivity, and the reduction from the asymptotic capacity to a single-letter formula—are both crucial to the elegance of Shannon's theory. The latter allows us to compute capacities, and the former tells

*toby.cubitt@bristol.ac.uk
†chenkenshin@gmail.com
‡a.harrow@bris.ac.uk

us that this single number completely characterises the channel's usefulness for classical information transmission.

Accordingly, in quantum information theory the most important questions in extending Shannon's techniques concern *additivity* (whether the capacity of two channels together is ever greater than the sum of their individual capacities) and *regularisation* (whether the asymptotic capacity of a channel can be reduced to optimising an entropic quantity over a single use of a channel). The classical and quantum capacities of a quantum channel can be expressed in terms of the regularised asymptotic limits of the *Holevo capacity* [1, 2] and *coherent information* [3, 4, 5], respectively. There was an early hope that the quantum capacity of a quantum channel might be expressed in terms of the maximum coherent information from a *single* use of the channel, and that the classical capacity could be similarly expressed in terms of the Holevo capacity. However, this hope proved to be unfounded. The maximum coherent information and Holevo capacity turn out not to equal the channel capacities. This was proved over a decade ago for the quantum capacity [6], and only in the last year for the classical capacity [7] (the culmination of a series of similar results [8, 9] for minimum output Rènyi entropies). This implies that entangling inputs across different channel uses is in general necessary for optimal quantum channel coding. It also tells us that if single-letter formulae exist for the quantum and classical capacities, they will not equal the maximum coherent information or the Holevo capacity.

However, these results tell us only that regularisation is necessary for our existing formula, not that the quantum channel capacities are necessarily non-additive. The first demonstration of non-additivity was given recently by Smith and Yard [10], who showed that the quantum capacity is super-additive. Indeed, their result proved that additivity is violated in the strongest possible sense: they exhibited two quantum channels which, individually, have zero quantum capacity. Yet, combine the two, and the joint channel has non-zero capacity. In other words, not only is the quantum capacity non-additive, there even exist channels that are completely useless for transmitting quantum information, but which *can* transmit quantum information when used together. The term "*super-activation*" was coined in Ref. [11] to describe this phenomenon, since the two channels somehow "activate" each other's hidden ability to transmit quantum information. More recent work has established the nonadditivity of the private classical capacity [12, 13]. On the other hand, additivity of the classical capacity of a quantum channel remains an open question.

The Shannon capacity, and the classical and quantum capacities mentioned so far, all measure the capacity for transmitting information with an error probability that can be made arbitrarily small, in the limit of arbitrarily many uses of the channel. Right from the early days of his development of classical information theory, Shannon also considered the *zero-error capacity*: the capacity of a channel to transmit information perfectly, with zero probability of error [14]. The zero-error capacity is important for applications in which no error can be tolerated, and also, and perhaps more importantly, when only a limited number of uses of the channel are available, so that the low error probability for the Shannon capacity can not be achieved.

Even in the case of classical channels, the zero-error capacity turns out to be mathematically very different to the standard Shannon capacity. For example, it is known to be non-additive. (See e.g. Ref. [15] for a review of zero-error

information theory.) However, it is not difficult to see that there can be no superactivation of the zero-error capacity of a classical channel. The main result of our paper shows that for *quantum* channels this is no longer true; the zero-error classical capacity of a quantum channel *can* be superactivated:

Theorem 1 *Let $d_A = 16, d_E = 4(2d_A - 1) = 124$ and $d_B = d_A d_E = 1984$. Then there exist channels $\mathcal{E}_1, \mathcal{E}_2$ such that:*

- *Each channel $\mathcal{E}_{1,2}$ maps $\mathbb{C}^{d_A}$ to $\mathbb{C}^{d_B}$ and has d_E Kraus operators.*
- *Each channel $\mathcal{E}_{1,2}$ has no zero-error capacity.*
- *The joint channel $\mathcal{E}_1 \otimes \mathcal{E}_2$* does *have non-zero zero-error capacity.*

In other words, there exist pairs of quantum channels that individually cannot be used for perfect transmission of *any* classical information at all, even if infinitely many uses of the channel are available. Yet, when the two channels are combined, even a *single* use of the each of the two channels allows perfect, error-free transmission of classical information. To our knowledge, this is the first example of superactivation of any kind of classical capacity of standard quantum channels.

Naturally, similar results also hold for larger-dimensional input and output spaces. Increasing the output dimension is trivial, since the channels do not need to make use of the entire output space. To increase the input dimension without changing the results of the theorem, we define channels $\hat{\mathcal{E}}_{1,2}$ that act as follows: on the first 16 dimensions of the input $\hat{\mathcal{E}}_{1,2}$ match the behaviour of $\mathcal{E}_{1,2}$, and the remaining dimensions are mapped to a maximally mixed state on the output.

The definition of zero-error capacity is easily extended to the quantum setting [16]. Beigi and Shor investigated the computational complexity of computing the zero-error capacity of quantum channels [17], showing that it is in general difficult to compute. Most notably, and one of the main inspirations for this work, Duan and Shi [18] proved a "one-shot" result in the case of multi-sender/multi-receiver quantum channels, when the senders and receivers are restricted to local operations and classical communication (LOCC). They exhibited examples of such channels for which a *single use* has no zero-error classical capacity but two uses do have non-zero zero-error capacity.

Duan and Shi's work hints at superactivation of the asymptotic capacity for standard quantum channels. Indeed, it raises two tantalising questions. Are these remarkable properties of the zero-error capacity inherent to communication over quantum channels, or do they arise from the LOCC constraints in the multi-sender/multi-receiver setting, which are crucial for their proofs? Furthermore, are their results an artifact of the one-shot case, that would disappear in the asymptotic setting? Both questions are compellingly answered by our work. This paper is also in some sense a sequel to our earlier work in Ref. [9], which demonstrated non-multiplicativity of the one-shot minimum output rank of a quantum channel, and its extension to the asymptotic case in Ref. [19]. (The relation between this problem and the superactivation phenomenon will be explained in Section 4.)

The paper is organised as follows. Section 2 introduces the necessary notation and concepts, and Section 3 proves some basic mathematical properties of

composite quantum maps that play a key role later. In Section 4, we prove a one-shot version of the main result. This is presented in some detail because, firstly, the main result builds directly on techniques used to prove the one-shot case and, secondly, in the one-shot case we are able to give explicit examples which may give some insight into the main result. In Section 5, we draw on techniques from algebraic geometry to prove our main result: superactivation of the asymptotic zero-error classical capacity of quantum channels. Finally, we conclude in Section 6 with a discussion of the results and their implications.

2 Preliminaries

The complex conjugate of x will be denoted $\bar{x}$. The $*$–conjugate $\mathcal{E}^*$ of a map $\mathcal{E}$ on the space $\mathcal{B}(\mathcal{H})$ of bounded operators on $\mathcal{H}$ is the dual with respect to the Hilbert-Schmidt inner-product, i.e. the unique map defined by

$$\mathrm{Tr}[A^\dagger\,\mathcal{E}(B)] = \mathrm{Tr}[\,\mathcal{E}^*(A)^\dagger\,B]. \tag{1}$$

A map $\mathcal{E}$ on $\mathcal{B}(\mathcal{H})$ is *completely positive* (CP) if it not only maps all positive operators to positive operators, but also preserves positivity when applied to a subsystem of some larger system. A CP map is completely positive and *trace-preserving* (CPT) if it in addition preserves the trace of operators. (CPT maps in quantum mechanics play exactly the analogous role to communication channels in classical information theory, and we will use the terms *quantum channel* and CPT map synonymously.)

The "flip" operation on a bipartite state is the composition of the swap operation, which interchanges the two parties, and complex conjugation:

$$\mathbb{F}(|\psi\rangle_{AB}) = \mathrm{SWAP}(|\bar{\psi}\rangle_{AB}). \tag{2}$$

(Note that the complex conjugation means the flip operation is basis-dependent; the computational product basis should be assumed when no basis is stated explicitly.) Thus, with complex-conjugation defined in the computational basis,

$$\mathbb{F}\Big(\sum_{ij} c_{ij}\,|i\rangle_A\,|j\rangle_B\Big) = \sum_{ij} \bar{c}_{ij}\,|j\rangle_A\,|i\rangle_B\,. \tag{3}$$

The definition of the flip operation extends to operators as $\mathbb{F}(M) = \mathrm{SWAP}\cdot\bar{M}\cdot\mathrm{SWAP}$.

Definition 2 *We say that a bipartite state or operator is* conjugate-symmetric *in a given basis if it is invariant under the flip operation, and similarly for a subspace invariant under the same operation.*

There is a natural isomorphism between (unnormalised) states $|\psi\rangle_{AB}$ in a bipartite space $\mathbb{C}^{d_A}\otimes\mathbb{C}^{d_B}$ and $d_A\times d_B$ matrices M: writing $|\psi\rangle$ in a product basis, we have

$$|\psi\rangle_{AB} = \sum_{ij} M_{ij}\,|i\rangle\,|j\rangle\,. \tag{4}$$

We will write $\mathbb{M}(|\psi\rangle)$ when we wish to denote the coefficient matrix M corresponding to the state $|\psi\rangle$. Similarly, we denote by $\mathbb{M}(S)$ the matrix subspace isomorphic in this way to a subspace $S\subseteq\mathcal{H}_A\otimes\mathcal{H}_B$. In terms of these coefficient

matrices, a conjugate-symmetric state is one for which $\mathbb{M}(|\psi\rangle)$ is Hermitian, and a subspace is conjugate-symmetric iff the corresponding matrix space is spanned by a basis of Hermitian matrices. Note that the *Schmidt-rank* of the state $|\psi\rangle$ is exactly the linear rank of $\mathbb{M}(|\psi\rangle)$.

Definition 3 *We say that a bipartite state $|\psi\rangle_{AB}$ is* positive-semidefinite *in a given product basis if $\mathbb{M}(|\psi\rangle)$ is a positive-semidefinite matrix. (Note that this includes the statement that $\mathbb{M}(|\psi\rangle)$ is Hermitian.) Similarly, a positive-semidefinite subspace S_{AB} is one that admits a* basis *whose elements are all positive-semidefinite.*

Note that it is obviously *not* the case that all elements of a positive-semidefinite subspace $\mathbb{M}(S_{AB})$ need themselves be positive-semidefinite, just that there exists *some* set of positive-semidefinite elements that span the space.

Definition 4 *We say a map $\mathcal{N}$ is* conjugate-divisible *if it can be decomposed as $\mathcal{N} = \mathcal{E}^* \circ \mathcal{E}$ for some CPT map $\mathcal{E}$.*

It will frequently be convenient to work with the Choi-Jamiołkowski representation of a map. Recall that the Choi-Jamiołkowski matrix associated with a map $\mathcal{E}$ is the matrix $\sigma_{AB} = \mathcal{I}_A \otimes \mathcal{E}_B(\omega_{AB})$ obtained by applying the map to one half of the (unnormalised) full Schmidt-rank state $|\omega\rangle = \sum_i \lambda_i |\varphi_i\rangle_A |\chi_i\rangle_B$. This isomorphism holds regardless of whether $\mathcal{E}$ is a CPT map or not; iff $\mathcal{E}$ is CP(T), then σ is a (trace 1) positive operator. (The standard Choi-Jamiołkowski matrix $\tilde{\sigma}_{AB}$ is obtained by setting $|\omega\rangle = \sum_i |i\rangle |i\rangle$, but the isomorphism holds more generally.) Introducing the unitary basis change $U|\varphi_i\rangle = |\chi_i\rangle$, We can recover the action of the map $\mathcal{E}$ from the matrix σ_{AB} via

$$\mathcal{E}(\rho) = \mathrm{Tr}_A \left[U \sigma_A^{-1/2} \sigma_{AB}\, \sigma_A^{-1/2} U^\dagger \cdot \rho^T \otimes \mathbb{1} \right], \tag{5}$$

where $\sigma_A = \mathrm{Tr}_A[\sigma_{AB}]$. For the standard Choi-Jamiołkowski matrix $\tilde{\sigma}_{AB}$, this simplifies to $\mathcal{E}(\rho) = \mathrm{Tr}_A[\,\tilde{\sigma}_{AB} \cdot \rho^T \otimes \mathbb{1}]$, and the non-standard Choi-Jamiołkowski matrix σ_{AB} is related to the standard one by rotating and rescaling the A subsystem:

$$\tilde{\sigma}_{AB} = U \sigma_A^{-1/2} \sigma_{AB}\, \sigma_A^{-1/2} U^\dagger. \tag{6}$$

3 Conjugate-divisible maps

The composite map $\mathcal{E}^* \circ \mathcal{E}$ will turn out to play a key role in studying the zero-error capacity of the channel $\mathcal{E}$. So we will first need to establish some basic properties of such conjugate-divisible maps. The main goal is a complete characterisation of their Choi-Jamiołkowski matrices.

Lemma 5 *If ρ_{AB} is the (standard) Choi-Jamiołkowski matrix for a channel $\mathcal{E}$, then the Choi-Jamiołkowski matrix of $\mathcal{E}^*$ is given by $\mathbb{F}(\rho_{AB}) = \bar{\rho}_{BA}$.*

Proof We have

$$\begin{aligned}
\mathrm{Tr}\left[\mathcal{E}^*(\psi)^\dagger\,\varphi\right] &= \mathrm{Tr}\left[\psi^\dagger\,\mathcal{E}(\varphi)\right] && \text{(7a)}\\
&= \mathrm{Tr}\left[\psi^\dagger\ \mathrm{Tr}_A\left(\rho_{AB}\cdot\varphi^T\otimes\mathbb{1}\right)\right] && \text{(7b)}\\
&= \mathrm{Tr}\left[\mathbb{1}\otimes\psi^\dagger\cdot\rho_{AB}^{T_A}\cdot\varphi\otimes\mathbb{1}\right] && \text{(7c)}\\
&= \mathrm{Tr}\left[\mathrm{Tr}_B\left(\mathbb{1}\otimes\psi\cdot\bar{\rho}_{AB}^{T_B}\right)^\dagger\cdot\varphi\right] && \text{(7d)}\\
&= \mathrm{Tr}\left[\mathrm{Tr}_B\left(\bar{\rho}_{BA}^{T_B}\cdot\psi\otimes\mathbb{1}\right)^\dagger\cdot\varphi\right] && \text{(7e)}\\
&= \mathrm{Tr}\left[\mathrm{Tr}_B\left(\mathbb{F}(\rho_{AB})\cdot\psi^T\otimes\mathbb{1}\right)^\dagger\cdot\varphi\right], && \text{(7f)}
\end{aligned}$$

from which we identify the Choi-Jamiołkowski matrix for $\mathcal{E}^*$ to be as claimed.□

Lemma 6 *If ρ_{AB} is the (standard) Choi-Jamiołkowski matrix for a channel $\mathcal{E}$, then the Choi-Jamiołkowski matrix of $\mathcal{N}=\mathcal{E}^*\circ\mathcal{E}$ is given by*

$$\sigma_{AA'} = \mathrm{Tr}_B\left[\rho_{AB}\otimes\mathbb{1}_{A'}\cdot\mathbb{1}_A\otimes\bar{\rho}_{BA'}^{T_B}\right]. \tag{8}$$

Proof We have

$$\begin{aligned}
\mathcal{N}(\psi) &= \mathrm{Tr}_B\left[\bar{\rho}_{BA'}\cdot\mathrm{Tr}_A\left(\rho_{AB}\cdot\psi^T\otimes\mathbb{1}_B\right)^T\otimes\mathbb{1}_{A'}\right] && \text{(9a)}\\
&= \mathrm{Tr}_B\left[\mathrm{Tr}_A\left(\rho_{AB}\cdot\psi^T\otimes\mathbb{1}_B\right)\otimes\mathbb{1}_{A'}\cdot\bar{\rho}_{BA'}^{T_B}\right] && \text{(9b)}\\
&= \mathrm{Tr}_A\left[\mathrm{Tr}_B\left(\rho_{AB}\otimes\mathbb{1}_{A'}\cdot\mathbb{1}_A\otimes\bar{\rho}_{BA'}^{T_B}\right)\cdot\psi^T\otimes\mathbb{1}_{A'}\right], && \text{(9c)}
\end{aligned}$$

from which we identify the Choi-Jamiołkowski matrix of $\mathcal{N}$ to be as claimed.□

The following extension to non-standard Choi-Jamiołkowski matrices follows immediately.

Corollary 7 *If ρ_{AB} is a non-standard Choi-Jamiołkowski matrix for a channel $\mathcal{E}$, related to the standard Choi-Jamiołkowski matrix by*

$$\tilde{\rho}_{AB} = U\rho_A^{-1/2}\rho_{AB}\,\rho_A^{-1/2}U^\dagger, \tag{10}$$

then

$$\sigma_{AA'} = \mathrm{Tr}_B\left[\rho_{AB}\otimes\mathbb{1}_{A'}\cdot\mathbb{1}_A\otimes\bar{\rho}_{BA'}^{T_B}\right] \tag{11}$$

can be viewed as a non-standard Choi-Jamiołkowski matrix for $\mathcal{N}=\mathcal{E}^*\circ\mathcal{E}$ by identifying it with the standard Choi-Jamiołkowski matrix $\tilde{\sigma}_{AA'}$ for $\mathcal{N}$ in the following way:

$$\tilde{\sigma}_{AA'} = U\sigma_A^{-1/2}\otimes\bar{U}\bar{\sigma}_{A'}^{-1/2}\cdot\sigma_{AA'}\cdot\sigma_A^{-1/2}U^\dagger\otimes\bar{\sigma}_{A'}^{-1/2}\bar{U}^\dagger. \tag{12}$$

With these basic properties in hand, we are now in a position to prove a necessary condition for a matrix to be the Choi-Jamiołkowski matrix of some conjugate-divisible map.

Proposition 8 *The support of the Choi-Jamiołkowski matrix of a conjugate-divisible map is both conjugate-symmetric and positive-semidefinite.*

Proof To establish conjugate-symmetry, let $\mathcal{N} = \mathcal{E}^* \circ \mathcal{E}$ be conjugate-divisible, where $\mathcal{E} : A \to B$ is CPT, and denote the (standard) Choi-Jamiołkowski matrix of $\mathcal{E}$ by ρ_{AB}. By Lemma 6, the Choi-Jamiołkowski matrix of $\mathcal{N}$ is given by

$$\sigma_{AA'} = \operatorname{Tr}_B \left[\rho_{AB} \otimes \mathbb{1}_{A'} \cdot \mathbb{1}_A \otimes \bar{\rho}_{BA'}^{T_B}\right]. \tag{13}$$

Hence

$$\begin{aligned}
\mathbb{F}(\sigma_{AA'}) &= \mathbb{F}\left(\operatorname{Tr}_B \left[\rho_{AB} \otimes \mathbb{1}_{A'} \cdot \mathbb{1}_A \otimes \bar{\rho}_{BA'}^{T_B}\right]\right) && \text{(14a)}\\
&= \operatorname{Tr}_B \left[\mathbb{1}_A \otimes \bar{\rho}_{BA'} \cdot \rho_{AB}^{T_B} \otimes \mathbb{1}_{A'}\right] && \text{(14b)}\\
&= \operatorname{Tr}_B \left[\rho_{AB} \otimes \mathbb{1}_{A'} \cdot \mathbb{1}_A \otimes \bar{\rho}_{BA'}^{T_B}\right] && \text{(14c)}\\
&= \sigma_{AA'}. && \text{(14d)}
\end{aligned}$$

Since $\sigma_{AA'}$ is conjugate-symmetric, so is its support (i.e. the support is invariant as a subspace under the action of $\mathbb{F}$).

To establish positive-semidefiniteness, first write the eigenvectors $|\varphi_k\rangle$ of ρ_{AB} in a product basis:

$$\rho_{AB} = \sum_k |\varphi_k\rangle\langle\varphi_k|\,, \qquad |\varphi_k\rangle_{AB} = \sum_i |\psi_i^k\rangle_A\, |i\rangle_B\,, \tag{15}$$

where the eigenvalues and coefficients have been absorbed into the unnormalised states $|\varphi_k\rangle_{AB}$ and $|\psi_i^k\rangle_A$ (note also that $|\psi_i^k\rangle_A$ are not necessarily orthogonal). Then

$$\begin{aligned}
\sigma_{AA'} &= \operatorname{Tr}_B \left[\rho_{AB} \otimes \mathbb{1}_{A'} \cdot \mathbb{1}_A \otimes \bar{\rho}_{BA'}^{T_B}\right] && \text{(16a)}\\
&= \operatorname{Tr}_B \left[\sum_{ijk} |\psi_i^k\rangle\, |i\rangle\, \langle\psi_j^k|\, \langle j| \otimes \mathbb{1}_{A'} \cdot \mathbb{1}_A \otimes \sum_{lmn} |n\rangle\, |\bar{\psi}_m^l\rangle\, \langle m|\, \langle\bar{\psi}_n^l|\right] && \text{(16b)}\\
&= \sum_{ijkl} |\psi_i^k\rangle\, |\bar{\psi}_i^l\rangle\, \langle\psi_j^k|\, \langle\bar{\psi}_j^l| && \text{(16c)}\\
&= \sum_{kl} \Big(\sum_i |\psi_i^k\rangle\, |\bar{\psi}_i^l\rangle\Big)\Big(\sum_j \langle\psi_j^k|\, \langle\bar{\psi}_j^l|\Big), && \text{(16d)}
\end{aligned}$$

from which we see that

$$S_{AA'} = \operatorname{supp}(\sigma_{AA'}) = \operatorname{span}\Big\{\sum_i |\psi_i^k\rangle\, |\bar{\psi}_i^l\rangle\Big\}_{k,l}. \tag{17}$$

Now, as matrices

$$\mathbb{M}\Big(\sum_i |\psi_i^k\rangle\, |\bar{\psi}_i^l\rangle\Big) = \sum_i |\psi_i^k\rangle\, \langle\psi_i^l|\,, \tag{18}$$

which are supported on $\operatorname{span}\{|\psi_i^k\rangle\}$. In particular, the matrix subspace $\mathbb{M}(S_{AA'})$ contains

$$\mathbb{M}\Big(\sum_{ik} |\psi_i^k\rangle\, |\bar{\psi}_i^k\rangle\Big) = \sum_{ik} |\psi_i^k\rangle\, \langle\psi_i^k| \tag{19}$$

which has full support on the subspace $\mathrm{span}\{|\psi_i^k\rangle\}$ and, being a sum of (unnormalised) projectors, has positive eigenvalues on that subspace. Thus we can choose as a basis for $\mathbb{M}(S_{AA'})$ the set of matrices

$$\Big\{\sum_j \Big(|\psi_j^k\rangle\langle\psi_j^l| + |\psi_j^l\rangle\langle\psi_j^k|\Big) + c\sum_{j,k}|\psi_j^k\rangle\langle\psi_j^k|\,,\\ \sum_j i\Big(|\psi_j^k\rangle\langle\psi_j^l| - |\psi_j^l\rangle\langle\psi_j^k|\Big) + c\sum_{j,k}|\psi_j^k\rangle\langle\psi_j^k|\Big\}_{k,l} \tag{20a}$$

which are all Hermitian and, for sufficiently large c, positive-semidefinite. □

We now show that the necessary conditions of Proposition 8 are also sufficient.

Proposition 9 *For any conjugate-symmetric, positive-semidefinite subspace $S_{AA'}$ which has full support on the first subsystem (i.e.* $\mathrm{supp}(\mathrm{Tr}_{A'}[S_{AA'}]) = \mathcal{H}_A$*), we can construct a (in general non-standard) Choi-Jamiołkowski matrix $\sigma_{AA'}$ of a conjugate-divisible map such that* $\mathrm{supp}(\sigma_{AA'}) = S_{AA'}$. *The corresponding channel $\mathcal{E}$ has input dimension d_A, rank $d_E = \dim S_{AA'}$ and output dimension $d_B = d_A d_E$.*

(Here, $\mathrm{supp}(\mathrm{Tr}_{A'}[S_{AA'}])$ is shorthand for $\bigcup_{|\psi\rangle\in S_{AA'}}\mathrm{supp}(\mathrm{Tr}_{A'}|\psi\rangle\langle\psi|)$. The condition on the support is necessary for a matrix to be any kind of Choi-Jamiołkowski matrix, simply by definition.)

Proof Since $S_{AA'}$ is positive-semidefinite, we can choose a Hermitian basis $\{M_k\}$ for $\mathbb{M}(S_{AA'})$ such that $M_k \geq 0$. Writing M_k in its spectral decomposition,

$$M_k = \sum_i |\psi_i^k\rangle\langle\psi_i^k|\,, \tag{21}$$

where we have absorbed the (positive) eigenvalues into the unnormalised eigenstates $|\psi_i^k\rangle$, we have

$$S_{AA'} = \mathrm{span}\Big\{\sum_i |\psi_i^k\rangle|\bar{\psi}_i^k\rangle\Big\}_k \tag{22}$$

and $\mathcal{H}_A = \mathrm{span}\{|\psi_i^k\rangle\}$.

Now consider the operator

$$\rho_{AB} = \sum_{ijk}|\psi_i^k\rangle_A|k,i\rangle_B\langle\psi_j^k|_A\langle k,j|_B\,. \tag{23}$$

This is Hermitian, positive-semidefinite, and $\mathrm{Tr}_B[\rho_{AB}]$ is full rank on $\mathcal{H}_A$, so (up to normalisation) ρ_{AB} is a (non-standard) Choi-Jamiołkowski matrix corresponding to some CPT map $\mathcal{E}$. Observe also that the rank and local dimensions

of ρ_{AB} are as claimed in the statement of the proposition. By Corollary 7,

$$\sigma_{AA'} = \mathrm{Tr}_B\left[\rho_{AB} \otimes \mathbb{1}_A \cdot \mathbb{1}_A \otimes \bar{\rho}_{BA'}^{T_B}\right] \tag{24a}$$

$$= \mathrm{Tr}_B\left[\sum_{ijk} |\psi_i^k\rangle |k,i\rangle \langle\psi_j^k| \langle k,j| \otimes \mathbb{1}_{A'} \cdot \mathbb{1}_A \otimes \sum_{lmn} |l,n\rangle |\psi_m^l\rangle \langle l,m| \langle\psi_n^l|\right] \tag{24b}$$

$$= \sum_k \Big(\sum_i |\psi_i^k\rangle |\bar{\psi}_i^k\rangle\Big)\Big(\sum_j \langle\psi_j^k| \langle\bar{\psi}_j^k|\Big) \tag{24c}$$

is a (non-standard) Choi-Jamiołkowski matrix for the conjugate-divisible channel $\mathcal{E}^* \circ \mathcal{E}$. Clearly, the support of this operator is $S_{AA'}$, so it fulfils the requirements of the proposition. □

Propositions 8 and 9 together imply the following key theorem, giving a complete characterisation of the Choi-Jamiołkowski matrices of conjugate-divisible maps.

Theorem 10 *Given a subspace $S_{AA'}$ such that $\mathrm{supp}(\mathrm{Tr}_{A'}[S_{AA'}]) = \mathcal{H}_A$, there exists a conjugate-divisible map with (in general non-standard) Choi-Jamiołkowski matrix $\sigma_{AA'}$ such that $\mathrm{supp}(\sigma_{AA'}) = S_{AA'}$ iff $S_{AA'}$ is conjugate-divisible and positive-semidefinite.*

4 Superactivation of the One-Shot Zero-Error Capacity

The *zero-error classical capacity* of a quantum channel is the capacity to transmit classical information with zero probability of error (as opposed to a vanishing error probability, as in the usual Shannon capacity; for brevity, we will drop the "classical" nomenclature from now on, and call this simply the *zero-error capacity*). The *one-shot zero-error capacity* is the amount of (classical) information that can be transmitted with zero probability of error by a *single* use of the channel (as opposed to the asymptotic rate per use of the channel in the limit of infinitely many uses of the channel). Our aim in this section is to show that there exist two quantum channels, which individually have zero one-shot zero-error capacity, but whose joint channel *does* have a non-zero zero-error capacity. (In Section 5, we will extend this result to the asymptotic capacity.)

A channel $\mathcal{E}$ has non-zero (one-shot) zero-error capacity if there exist two different input states whose outputs are perfectly distinguishable. In other words, the one-shot zero-error capacity is non-zero iff

$$\exists\, |\psi\rangle, |\varphi\rangle \in \mathcal{H}_A : \mathrm{Tr}[\mathcal{E}(\psi)^\dagger \mathcal{E}(\varphi)] = 0. \tag{25}$$

Note that

$$\mathrm{Tr}[\mathcal{E}(\psi)^\dagger \mathcal{E}(\varphi)] = \mathrm{Tr}[\psi \cdot \mathcal{E}^*\big(\mathcal{E}(\varphi)\big)] = \mathrm{Tr}[\psi \cdot \mathcal{E}^* \circ \mathcal{E}(\varphi)]. \tag{26}$$

Conversely, a channel has zero one-shot zero-error capacity iff

$$\forall\, |\psi\rangle, |\varphi\rangle \in \mathcal{H}_A : \mathrm{Tr}[\psi \cdot \mathcal{E}^* \circ \mathcal{E}(\varphi)] \neq 0. \tag{27}$$

Thus we seek two channels, $\mathcal{E}_1$ and $\mathcal{E}_2$, such that

$$\forall \left|\psi\right\rangle, \left|\varphi\right\rangle \in \mathcal{H}_A : \mathrm{Tr}[\psi \cdot \mathcal{E}_{1,2}^* \circ \mathcal{E}_{1,2}(\varphi)] \neq 0, \tag{28a}$$

$$\exists \left|\psi\right\rangle, \left|\varphi\right\rangle \in \mathcal{H}_A^{\otimes 2} : \mathrm{Tr}[\psi \cdot (\mathcal{E}_1^* \circ \mathcal{E}_1) \otimes (\mathcal{E}_2^* \circ \mathcal{E}_2)(\varphi)] = 0. \tag{28b}$$

For the composite maps $\mathcal{N}_{1,2} = \mathcal{E}_{1,2}^* \circ \mathcal{E}_{1,2}$ these are precisely the conditions established in Ref. [9] for $\mathcal{N}_{1,2}$ to violate multiplicativity of the minimum output rank! The composite map $\mathcal{N} = \mathcal{E}^* \circ \mathcal{E}$ need not be CPT even if $\mathcal{E}$ is, but this does not substantially affect the methods developed in Ref. [9], which we will reuse here.

To establish necessary and sufficient conditions for the individual maps to satisfy Eq. (28a), we follow exactly the same arguments as in Ref. [9]. Let $\sigma_{1,2}$ denote Choi-Jamiołkowski matrices corresponding to the conjugate-divisible maps $\mathcal{N}_{1,2}$. Then, from Eq. (28a), we have

$$\forall \left|\psi\right\rangle, \left|\varphi\right\rangle \in \mathcal{H}_A : \mathrm{Tr}\left[\psi_{A'} \cdot \mathrm{Tr}_A(\sigma_{1,2} \cdot \varphi_A^T \otimes \mathbb{1}_{A'})\right] = \mathrm{Tr}\left[\sigma_{1,2} \cdot \varphi_A^T \otimes \psi_{A'}\right] \neq 0. \tag{29}$$

Note that this holds even if $\sigma_{1,2}$ are non-standard Choi-Jamiołkowski matrices, since using Corollary 7 any rescaling can be absorbed into φ and ψ:

$$\mathrm{Tr}\left[U\sigma_A^{-1/2} \otimes \bar{U}\bar{\sigma}_A^{-1/2} \cdot \sigma_{AA'} \cdot \sigma_A^{-1/2}U^\dagger \otimes \bar{\sigma}_A^{-1/2}\bar{U}^\dagger \cdot \varphi_A \otimes \psi_{A'}\right] \tag{30a}$$

$$= \mathrm{Tr}\left[\sigma_{AA'} \cdot \left(\sigma_A^{-1/2}U^\dagger\varphi_A U\sigma_A^{-1/2} \otimes \bar{\sigma}_A^{-1/2}\bar{U}^\dagger\psi_{A'}\bar{U}\bar{\sigma}_A^{-1/2}\right)\right] \tag{30b}$$

$$= \mathrm{Tr}\left[\sigma_{AA'} \cdot \varphi'_A \otimes \psi'_{A'}\right]. \tag{30c}$$

Therefore, if $S_{1,2} = \mathrm{supp}(\sigma_{1,2})$ denote the supports of the Choi-Jamiołkowski matrices, it is necessary and sufficient to require that their orthogonal complements contain no product states:

$$\nexists \left|\psi\right\rangle, \left|\varphi\right\rangle \in \mathcal{H}_A \ : \ \left|\psi\right\rangle \otimes \left|\varphi\right\rangle \in S_{1,2}^\perp. \tag{31}$$

To derive sufficient conditions for the joint map to satisfy Eq. (28b), we slightly generalise the argument of Ref. [9]. First, fix both states $\left|\psi\right\rangle$, $\left|\varphi\right\rangle$ in Eq. (28b) to be maximally entangled: $\left|\psi\right\rangle = U_{A_1} \otimes V_{A_2}\left|\omega\right\rangle$, $\left|\varphi\right\rangle = W_{A'_1} \otimes X_{A'_2}\left|\omega\right\rangle$, where $\left|\omega\right\rangle = \sum_i \left|i,i\right\rangle$ and U, V, W, X are unitary. Then

$$0 = \mathrm{Tr}\left[\psi_{A'_1A'_2} \cdot \mathcal{N}_1 \otimes \mathcal{N}_2(\varphi_{A_1A_2})\right] \tag{32a}$$

$$= \mathrm{Tr}\left[\psi_{A'_1A'_2} \cdot \mathrm{Tr}_{A_1A_2}\left[\sigma_1 \otimes \sigma_2 \cdot \varphi_{A_1A_2}^T \otimes \mathbb{1}_{A'_1A'_2}\right]\right] \tag{32b}$$

$$= \mathrm{Tr}\left[\sigma_1 \otimes \sigma_2 \cdot \varphi_{A_1A_2}^T \otimes \psi_{A'_1A'_2}\right] \tag{32c}$$

$$= \mathrm{Tr}\big[\sigma_1 \otimes \sigma_2 \cdot (\bar{U} \otimes \bar{V}\ \omega_{A_1A_2}^T\ U^T \otimes V^T) \otimes (W \otimes X\ \omega_{A'_1A'_2}\ W^\dagger \otimes X^\dagger)\big] \tag{32d}$$

$$= \mathrm{Tr}\left[(\bar{U} \otimes W\,\sigma_1\,U^T \otimes W^\dagger)^T \cdot (\bar{V} \otimes X\,\sigma_2\,V^T \otimes X^\dagger)\right] \tag{32e}$$

$$= \mathrm{Tr}\left[\sigma_1^T \cdot (U' \otimes V'\,\sigma_2\,{U'}^\dagger \otimes {V'}^\dagger)\right]. \tag{32f}$$

Again, this remains true if $\sigma_{1,2}$ are non-standard Choi-Jamiołkowski matrices, since we can absorb any rescaling into our choice of $\left|\psi\right\rangle$ and $\left|\varphi\right\rangle$. Writing

$U_{1,2}\sigma_{A_{1,2}}^{-1/2} = R_{1,2}$ for brevity, we have

$$\mathrm{Tr}\left[\psi_{A'_1A'_2} \cdot \mathcal{N}_1 \otimes \mathcal{N}_2(\varphi_{A_1A_2})\right] \tag{33a}$$
$$= \mathrm{Tr}\Big[\big(R_1 \otimes \bar{R}_1 \otimes R_2 \otimes \bar{R}_2\big) \cdot \sigma_{A_1A'_1} \otimes \sigma_{A_2A'_2} \cdot \big(R_1 \otimes \bar{R}_1 \otimes R_2 \otimes \bar{R}_2\big) \cdot \varphi^T_{A_1A_2} \otimes \psi_{A'_1A'_2}\Big] \tag{33b}$$
$$= \mathrm{Tr}\Big[\sigma_{A_1A'_1} \otimes \sigma_{A_2A'_2} \cdot (R_1 \otimes \bar{R}_1\, \varphi^T_{A_1A_2} R_1 \otimes \bar{R}_1) \otimes (R_2 \otimes \bar{R}_2\, \psi_{A'_1A'_2} R_2 \otimes \bar{R}_2)\Big] \tag{33c}$$
$$= \mathrm{Tr}\left[\sigma_{A_1A'_1} \otimes \sigma_{A_2A'_2} \cdot {\varphi'}^T_{A_1A_2} \otimes \psi'_{A'_1A'_2}\right]. \tag{33d}$$

Therefore, in terms of the supports $S_{1,2}$ of the Choi-Jamiołkowski matrices $\sigma_{1,2}$, Eq. (32f) implies that a sufficient condition for the maps to satisfy Eq. (28b) is for the supports to be related by

$$S_2^T = U \otimes V \cdot S_1^\perp \tag{34}$$

for some local unitaries U, V.

Of course, since $\mathcal{N}_{1,2} = \mathcal{E}^*_{1,2} \circ \mathcal{E}_{1,2}$ are necessarily conjugate-divisible, Theorem 10 also applies, so $S_{1,2}$ must also be conjugate-symmetric and positive-semidefinite. If we can find subspaces simultaneously satisfying these conditions *and* Eqs. (31) and (34), then by Theorem 10 we can construct channels $\mathcal{E}_{1,2}$ such that $\mathcal{N}_{1,2} = \mathcal{E}^*_{1,2} \circ \mathcal{E}_{1,2}$ satisfy Eqs. (28a) and (28b). (Note that w.l.o.g. we can neglect the condition in Theorem 10 that $\mathrm{supp}(\mathrm{Tr}_{A'}[S_{AA'}]) = \mathcal{H}_A$, since if this is not the case we can always shrink $\mathcal{H}_A$ so that it does hold.) Noting that Schmidt-rank, conjugate-symmetry and positive-semidefiniteness are preserved under the transpose operation, we can for convenience redefine $S_2 = \mathrm{supp}(\sigma_2^T)$ in Eq. (34) (without changing Eq. (31)) to save carrying the transpose around in the notation.

These results are summarised in the following lemma:

Lemma 11 *If there exist subspaces $S_1, S_2 \in \mathcal{H}_A \otimes \mathcal{H}_A$ satisfying*

$$\nexists\, |\psi\rangle, |\varphi\rangle \in \mathcal{H}_A : |\psi\rangle \otimes |\varphi\rangle \in S_{1,2}^\perp\,, \tag{35a}$$
$$S_2 = U \otimes V \cdot S_1^\perp, \tag{35b}$$
$$\mathbb{F}(S_{1,2}) = S_{1,2}\,, \tag{35c}$$
$$\exists \{M_i^{1,2} \geq 0\} : \mathbb{M}(S_{1,2}) = \mathrm{span}\{M_i^{1,2}\}, \tag{35d}$$

then there exist channels $\mathcal{E}_{1,2}$ which individually have zero one-shot zero-error capacity, but for which the joint channel $\mathcal{E}_1 \otimes \mathcal{E}_2$ has non-zero zero-error capacity.

If a subspace is conjugate-symmetric, then so is its orthogonal complement, so Eqs. (35b) and (35c) together imply

$$U \otimes V \cdot S_1 = S_2^\perp = \mathbb{F}(S_2^\perp) = \mathbb{F}(U \otimes V \cdot S_1). \tag{36}$$

Conversely, if Eq. (36) holds for conjugate-symmetric S_1, then clearly Eq. (35c) is satisfied. Thus, letting $S_1 = S$, $S_2 = U \otimes V \cdot S^\perp$, and recalling that Schmidt-rank is invariant under local-unitaries, Eqs. (35a) and (35c) can, respectively,

be re-expressed as:

$$\nexists\, |\psi\rangle\,, |\varphi\rangle \in \mathcal{H}_A : |\psi\rangle \otimes |\varphi\rangle \in S \text{ or } S^\perp, \tag{35a'}$$
$$\mathbb{F}(S) = S \;\text{ and }\; \mathbb{F}(U \otimes V \cdot S) = U \otimes V \cdot S. \tag{35c'}$$

We can therefore rewrite Lemma 11 in terms of a single subspace S:

Theorem 12 *If there exists a subspace $S \in \mathcal{H}_A \otimes \mathcal{H}_A$ satisfying*

$$\nexists\, |\psi\rangle\,, |\varphi\rangle \in \mathcal{H}_A : |\psi\rangle \otimes |\varphi\rangle \in S^\perp, \tag{37a}$$
$$\nexists\, |\psi\rangle\,, |\varphi\rangle \in \mathcal{H}_A : |\psi\rangle \otimes |\varphi\rangle \in S, \tag{37b}$$
$$\mathbb{F}(S) = S\,, \tag{37c}$$
$$\mathbb{F}(U \otimes V \cdot S) = U \otimes V \cdot S, \tag{37d}$$
$$\exists\{M_i \geq 0\} : \mathbb{M}(S) = \operatorname{span}\{M_i\}, \tag{37e}$$
$$\exists\{M_j \geq 0\} : \mathbb{M}(U \otimes V \cdot S^\perp) = \operatorname{span}\{M_j\}, \tag{37f}$$

then there exist channels $\mathcal{E}_{1,2}$ which individually have zero one-shot zero-error capacity, but for which the joint channel $\mathcal{E}_1 \otimes \mathcal{E}_2$ has non-zero zero-error capacity.

Our task, then, reduces to finding a subspace S which satisfies the conditions of Theorem 12. (The first two conditions are identical to those required in Ref. [9]. The remainder arise from the additional conjugate-divisibility requirement, which rules out the explicit example constructed in that paper.) Using the ideas of Refs. [9, 20], it is not too hard to find an explicit example of a subspace satisfying Theorem 12. For example, set

$$U = \mathbb{1}, \quad V = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix} =: X, \tag{38}$$

and choose the matrix subspace $\mathbb{M}(S_1)$ to be spanned by

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & & & \\ & i & & \\ & & -i & \\ & & & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & & & \\ & -i & & \\ & & i & \\ & & & -1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & & & 1 \\ & -1 & -1 & \\ & -1 & -1 & \\ 1 & & & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -4 & 7 & \\ & & & 7 \\ & & & -4 \\ & & & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & & & \\ -4 & & & \\ 7 & & & \\ & 7 & -4 & 0 \end{pmatrix}, \tag{39}$$
$$\begin{pmatrix} 0 & -8 & 9 & \\ & & & -9 \\ & & & 8 \\ & & & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & & & \\ -8 & & & \\ 9 & & & \\ & -9 & 8 & 0 \end{pmatrix}.$$

(The entries of the final four matrices are fairly arbitrary; they were essentially chosen by picking two different sets of four integers at random, and symmetrising.)

$\mathbb{M}(S_1^\perp)$ is then spanned by

$$\begin{pmatrix} & & & 1\\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix}, \quad \begin{pmatrix} & & & 1\\ & & i & \\ & -i & & \\ -1 & & & \end{pmatrix}, \quad \begin{pmatrix} & & & 1\\ & & -i & \\ & i & & \\ -1 & & & \end{pmatrix},$$
$$\begin{pmatrix} 1 & & & 1\\ & 1 & -1 & \\ & -1 & 1 & \\ 1 & & & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 2 & \\ & & & -6\\ & & & -8\\ & & & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & & & \\ 1 & & & \\ 2 & & & \\ & -6 & -8 & 0 \end{pmatrix}, \tag{40}$$
$$\begin{pmatrix} 0 & -8 & -6 & \\ & & & 2\\ & & & 1\\ & & & 0 \end{pmatrix}, \begin{pmatrix} 0 & & & \\ -8 & & & \\ -6 & & & \\ & 2 & 1 & 0 \end{pmatrix}.$$

It is straightforward to verify that this choice of S_1 satisfies the conjugate-symmetry conditions of Eqs. (37c) and (37d). To see that the positive-semi-definiteness conditions of Eqs. (37e) and (37f) are satisfied, note that S_1 and $\mathbb{1} \otimes X \cdot S_1^\perp$ both contain the identity matrix, which is positive and full rank. Thus we can construct a positive-semidefinite basis by adding sufficient weight of the identity to the other basis elements. Finally, the easiest way to prove that Eqs. (37a) and (37b) are satisfied is to use a computer algebra package such as Mathematica, and apply the Groebner basis algorithm. (Note that this provides a rigorous computer-aided proof, not merely supporting numerical evidence.)

5 Superactivation of the Asymptotic Zero-Error Capacity

We have proven in the previous section that the one-shot zero-error capacity can be superactivated, which hints at an even more remarkable possibility: can the *asymptotic* capacity be superactivated?

The main challenge lies in showing that a channel has zero zero-error capacity even in the asymptotic limit. This involves proving that *all* tensor powers of the channel have zero zero-error capacity. From the arguments of Section 4, this implies that the orthogonal complement of any tensor power of the support of its Choi-Jamiołkowski matrix should contain no product states. Thus, as in Section 4, our task is to find a subspace that satisfies all the conditions of Eqs. (37), but we strengthen Eqs. (37a) and (37b) to in addition require that no tensor powers of the subspaces contain any product states. Given such a subspace, we can construct a pair of channels in exactly the same way as we did in Section 4, but thanks to these stronger properties the individual channels will now have zero zero-error capacity even in the asymptotic limit. This is summarised in the following counterpart to Theorem 12.

Theorem 13 *If there exists a subspace S satisfying*

$$\forall k, \nexists \left|\psi\right\rangle, \left|\varphi\right\rangle \in \mathcal{H}_A^{\otimes k} : \left|\psi\right\rangle \otimes \left|\varphi\right\rangle \in (S^{\otimes k})^{\perp}, \tag{41a}$$

$$\forall k, \nexists \left|\psi\right\rangle, \left|\varphi\right\rangle \in \mathcal{H}_A^{\otimes k} : \left|\psi\right\rangle \otimes \left|\varphi\right\rangle \in \left((S^{\perp})^{\otimes k}\right)^{\perp}, \tag{41b}$$

$$\mathbb{F}(S) = S\,, \tag{41c}$$

$$\mathbb{F}(U \otimes V \cdot S) = U \otimes V \cdot S, \tag{41d}$$

$$\exists \{M_i \geq 0\} : \mathbb{M}(S) = \operatorname{span}\{M_i\}, \tag{41e}$$

$$\exists \{M_j \geq 0\} : \mathbb{M}(U \otimes V \cdot S^{\perp}) = \operatorname{span}\{M_j\}, \tag{41f}$$

then there exist channels $\mathcal{E}_{1,2}$ which individually have no zero-error capacity, but whose joint channel $\mathcal{E}_1 \otimes \mathcal{E}_2$ does *have non-zero zero-error capacity.*

Before proving that such a subspace exists, it is worth outlining the general approach. We first adapt and extend the algebraic-geometry arguments of Ref. [19] to show that either almost all subspaces satisfying Eqs. (41c) and (41d) also satisfy Eq. (41a), or none of them do. Then, we construct a particular subspace that *does* satisfy Eqs. (41a), (41c) and (41d). Whilst that particular subspace certainly does *not* satisfy Eq. (41b), the fact that it exists shows that almost all subspaces satisfying Eqs. (41c) and (41d) must also satisfy Eq. (41a). And, by symmetry, this implies that almost all of them also satisfy Eq. (41b). Therefore, if we choose a subspace satisfying Eqs. (41c) and (41d) at random, it will almost-surely satisfy Eqs. (41a) and (41b). Finally, we show that there is a non-zero probability that such a randomly chosen subspace will also satisfy Eqs. (41e) and (41f), implying that a subspace satisfying all the conditions in Theorem 13 does exist.

5.1 Strongly unextendible conjugate-symmetric subspaces are full measure

We first require some terminology, notation and basic results relating to the first two conditions, Eqs. (41a) and (41b), of Theorem 13.

Definition 14 *A subspace $S \in \mathcal{H}_A \otimes \mathcal{H}_B$ is k-unextendible if $(S^{\otimes k})^{\perp}$ contains no product state in $\mathcal{H}_{A^{\otimes k}} \otimes \mathcal{H}_{B^{\otimes k}}$. A subspace is* strongly unextendible *if it is k-unextendible for all $k \geq 1$. Conversely, a subspace is k*-extendible *if it is not k-unextendible, and* extendible *if it is not strongly unextendible.*

$\mathrm{Gr}_d(V)$ denotes the Grassmannian of a vector space V (the set of all d-dimensional subspaces of V). The sets of k-extendible, extendible, and unextendible subspaces of dimension d will be denoted, respectively,

$$E_d^k(\mathcal{H}_A, \mathcal{H}_B) = \{S \in \mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) \,|\, S \text{ is } k\text{-extendible}\}, \tag{42}$$

$$E_d(\mathcal{H}_A, \mathcal{H}_B) = \{S \in \mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) \,|\, S \text{ is extendible}\}, \tag{43}$$

$$U_d(\mathcal{H}_A, \mathcal{H}_B) = \{S \in \mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) \,|\, S \text{ is unextendible}\}, \tag{44}$$

so that

$$U_d(\mathcal{H}_A, \mathcal{H}_B) = \Big(\bigcup_k E_d^k(\mathcal{H}_A, \mathcal{H}_B)\Big)^c, \tag{45}$$

i.e. U_d is the complement of the union over all E_d^k.

We start by proving that E_d^k is an algebraic set:

Lemma 15 *$E^k_d(\mathcal{H}_A, \mathcal{H}_B)$ is Zariski-closed in* $\mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) = \mathrm{Gr}_d(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$.

Proof Define the following two maps:

$$\phi_1 : \mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathrm{Gr}_{d^k}(\mathcal{H}_{A^{\otimes k}} \otimes \mathcal{H}_{B^{\otimes k}}) \text{ which maps } S \longmapsto S^{\otimes k}, \tag{46a}$$

$$\phi_2 : \mathrm{Gr}_d(\mathcal{H}_{A^{\otimes k}} \otimes \mathcal{H}_{B^{\otimes k}}) \to \mathrm{Gr}_{d_A^k d_B^k - d}(\mathcal{H}_{A^{\otimes k}} \otimes \mathcal{H}_{B^{\otimes k}}) \text{ which maps } S \longmapsto S^{\perp}. \tag{46b}$$

We then have

$$E^k_d(\mathcal{H}_A, \mathcal{H}_B) = \{S \in \mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) \,|\, \phi_2 \circ \phi_1(S) \cap \Sigma_{d_A^k-1, d_B^k-1} \neq \varnothing\} \tag{47}$$

where $\Sigma_{d_A^k-1, d_B^k-1}$ is the Segre variety. If we let

$$T = \{S \in \mathrm{Gr}_{d_A^k d_B^k - d^k}(\mathcal{H}_{A^{\otimes k}} \otimes \mathcal{H}_{B^{\otimes k}}) \,|\, S \cap \Sigma_{d_A^k-1, d_B^k-1} \neq \varnothing\} \tag{48}$$

then $E^k_d(\mathcal{H}_A, \mathcal{H}_B) = (\phi_2 \circ \phi_1)^{-1}(T)$. ϕ_1 and ϕ_2 are both proper morphisms, thus their composition is again a proper morphism, which implies that the pre-image $E^k_d(\mathcal{H}_A, \mathcal{H}_B) = (\phi_2 \circ \phi_1)^{-1}(T)$ is Zariski closed if T is Zariski closed.

In the next step, we will prove the general result that

$$R_d(\mathcal{H}_A, \mathcal{H}_B) = \{S \in \mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) \,|\, S \cap \Sigma_{d_A-1, d_B-1} \neq \varnothing\} \tag{49}$$

is Zariski closed, which will imply T is Zariski closed. Let

$$X = \{(\mathcal{S}, [v]) \,|\, \mathcal{S} \subset \mathcal{H}_A \otimes \mathcal{H}_B, [v] \in \Sigma_{d_A-1, d_B-1} \text{ and } v \in \mathcal{S}\}. \tag{50}$$

Then X is a subset of $\mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) \times \Sigma_{d_A-1, d_B-1}$. Let P be the projection from $\mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) \times \Sigma_{d_A-1, d_B-1}$ to $\mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B)$, so that that $R_d(\mathcal{H}_A, \mathcal{H}_B) = P(X)$. It is not hard to check that X is Zariski closed. Since Σ_{d_A-1, d_B-1} is a projective variety it is complete, and as a result the image of projection P on any Zariski-closed set in $\mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_B) \times \Sigma_{d_A-1, d_B-1}$ is again Zariski closed. Therefore $R_d(\mathcal{H}_A, \mathcal{H}_B) = P(X)$ is Zariski closed. □

We will consider the case when $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^{d_A}$. In what follows, it will be useful to represent $\mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_A}$ as the real vector space $\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A}$. The complex Grassmannian $\mathrm{Gr}_d(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_A})$ can then be mapped injectively to the real Grassmannian $\mathrm{Gr}_{2d}(\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A})$. Define i to be a linear operator acting on $\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A}$ in the natural way, i.e. as $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \otimes \mathbb{1}_{d_A} \otimes \mathbb{1}_{d_A}$. Then $S \in \mathrm{Gr}_{2d}(\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A})$ corresponds to an element of $\mathrm{Gr}_d(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_A})$ if and only if it satisfies $iS = S$.

Now we use the fact that a Zariski-closed set in a complex vector space is also Zariski-closed in the isomorphic real vector space to obtain the following corollary to Lemma 15.

Corollary 16 *$E^k_{2d}(\mathcal{H}_A, \mathcal{H}_B)$ is Zariski-closed in the real Grassmannian* $\mathrm{Gr}_{2d}(\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{2d_B})$.

We now consider the set of subspaces that satisfy Eqs. (41c) and (41d) of Theorem 13. Denote this set by

$$F_d(\mathbb{C}, d_A) = \{S \in \mathrm{Gr}_d(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_A}) \,|\, S = \mathbb{F}(S),\ \mathbb{F}(U \otimes V \cdot S) = U \otimes V \cdot S\}. \tag{51}$$

To better handle the conjugate-linear constraints, we will consider the equivalent set of real vector spaces, defined to be

$$F_d(\mathbb{R}, d_A) = \{S \in \mathrm{Gr}_{2d}(\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A}) \mid \\ S = iS,\ S = \mathbb{F}(S),\ \mathbb{F}(U \otimes V \cdot S) = U \otimes V \cdot S\}. \quad (52)$$

While $F_d(\mathbb{R}, d_A)$ and $F_d(\mathbb{C}, d_A)$ are isomorphic, we will find it convenient to work with both of them at different times.

As the following lemma shows, this set is also algebraic:

Lemma 17 *$F_d(\mathbb{R}, d_A)$ is Zariski-closed in $\mathrm{Gr}_{2d}(\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A})$.*

Proof We will prove a more general statement. If $\mathcal{H}$ is a finite-dimensional real vector space, and $M \in \mathcal{B}(\mathcal{H})$ then define the action of M on $\mathrm{Gr}_d(\mathcal{H})$ by

$$M(S) = \{M\,|\psi\rangle : |\psi\rangle \in S\}, \quad (53)$$

for $S \in \mathrm{Gr}_d(\mathcal{H})$. Then we claim that the set of subspaces invariant under M, $\{S \in \mathrm{Gr}_d(\mathcal{H}) : M(S) = S\}$, is Zariski-closed in $\mathrm{Gr}_d(\mathcal{H})$.

To show the lemma follows from this claim, take $\mathcal{H} = \mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A}$ and M to be in turn i, $\mathbb{F}$, and $(U \otimes V) \cdot \mathbb{F}$. Then use the fact that the intersection of two Zariski-closed sets is also Zariski-closed.

To prove our claim about $\{S \in \mathrm{Gr}_d(\mathcal{H}) : M(S) = S\}$, we will use the Plücker embedding [21]. The Plücker embedding ι is a map from $\mathrm{Gr}_d(\mathcal{H})$ into $\mathbb{P}(\wedge^d \mathcal{H})$. Here $\wedge^d \mathcal{H}$ denotes the d^{th} exterior power of $\mathcal{H}$, and $\mathbb{P}$ indicates that we are taking the projectification of $\wedge^d \mathcal{H}$. If S is spanned by $\{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$ then $\iota(S)$ is defined to be $|\psi_1\rangle \wedge \ldots \wedge |\psi_d\rangle$. To see that ι is a well-defined map, observe that replacing $|\psi_i\rangle$ by $\sum_{j=1}^d A_{i,j}\,|\psi_j\rangle$ for an invertible matrix A has the effect of replacing $\iota(S)$ by $\det(A)\iota(S)$, which in projective space makes no difference.

The exterior product $|\psi_1\rangle \wedge \ldots \wedge |\psi_d\rangle$ can also be written as

$$\sum_{\sigma \in \mathcal{S}_d} (-1)^{\mathrm{sgn}(\sigma)}\,|\psi_{\sigma(1)}\rangle \otimes \cdots \otimes |\psi_{\sigma(d)}\rangle \quad (54)$$

where $\mathcal{S}_d$ is the symmetric group on d elements and $\mathrm{sgn}(\sigma)$ is the sign of the permutation σ. In this picture we have

$$\iota\big(M(S)\big) = M^{\otimes d}\,\iota(S). \quad (55)$$

Thus the condition that $M(S) = S$ is equivalent to demanding that $\iota(S) = M^{\otimes d}\,\iota(S)$. This is a linear constraint on $\iota(S)$, so $\{\iota(S) : \iota(S) = M^{\otimes d}\,\iota(S)\} = \{\iota(S) : M(S) = S\}$ is Zariski-closed. But ι is a proper morphism, so $\{S : M(S) = S\}$ must also be Zariski-closed, which completes the proof. □

The following follows immediately from Corollary 16 and Lemma 17:

Corollary 18 *$E_d^k(\mathcal{H}_A, \mathcal{H}_{A'}) \cap F_d(\mathbb{R}, d_A)$ is Zariski-closed in $F_d(\mathbb{R}, d_A)$.*

Any Zariski-closed subset has zero measure (in the usual Haar measure), unless it is the full space. Thus $\bigcup_k E_d^k$, which is a countable union of zero-measure sets, is either zero-measure or it is the full space. Conversely, since U_d is the complement of this union, it is either full measure or it is the empty set. Since the intersection of two Zariski-closed sets is Zariski-closed, the identical argument also holds for $E_d^k \cap F_d$ and $U_d \cap F_d$, hence:

Theorem 19 *If the set $U_d(\mathcal{H}_A, \mathcal{H}_{A'}) \cap F_d(\mathbb{R}, d_A) \neq \varnothing$, then it is full measure in $F_d(\mathbb{R}, d_A)$.*

5.2 Existence of a strongly unextendible conjugate-symmetric subspace

We now proceed to show that $U_d(\mathcal{H}_A, \mathcal{H}_{A'}) \cap F_d(\mathbb{R}, d_A)$ is not empty. We will do this by starting with a family of strongly unextendible subspaces and symmetrising them, so we need to get a handle on how much the symmetrisation blows up the dimension of the subspace, which is the content of the following lemma.

Lemma 20 *Let $\mathcal{F} : \mathrm{Gr}_d(\mathcal{H}_A \otimes \mathcal{H}_{A'}) \to \bigcup_{d'} F_{d'}(\mathbb{C}, d_A)$ be the map that symmetrises a subspace S by alternately iterating the maps $\mathcal{F}_1(S) = S + \mathbb{F}(S)$ and $\mathcal{F}_2(S) = S + \mathbb{F}_{U\otimes V}(S) = S + U^\dagger \otimes V^\dagger\, \mathbb{F}(U \otimes V \cdot S)$ until convergence. Then, for*

$$U = \mathbb{1}, \quad V = \begin{pmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \end{pmatrix} := X, \tag{56}$$

the dimension d' of the image $\mathcal{F}(S)$ satisfies $d' \leq 4d$.

Proof Let M be an element of $\mathbb{M}(S)$, and consider the action of $\mathbb{F}$ and $\mathbb{F}_{U\otimes V}$ on $\mathbb{M}(S)$. Since $X^\dagger = X$ and $X^2 = \mathbb{1}$, we have

$$\mathbb{F}(M) = M^\dagger, \tag{57}$$

$$\mathbb{F}_{U\otimes V}(M) = XM^\dagger X, \tag{58}$$

$$\mathbb{F} \circ \mathbb{F}(M) = \mathbb{F}_{U\otimes V} \circ \mathbb{F}_{U\otimes V}(M) = M, \tag{59}$$

$$\mathbb{F} \circ \mathbb{F}_{U\otimes V}(M) = \mathbb{F}_{U\otimes V} \circ \mathbb{F}(M) = XMX. \tag{60}$$

Thus the alternating application of $\mathcal{F}_1$ and $\mathcal{F}_2$ converges after a finite number of iterations, and maps a basis $\{M_i\}$ for $\mathbb{M}(S)$ to a basis $\{M_i, M_i^\dagger, XM_iX, XM_i^\dagger X\}$ for $\mathbb{M}(\mathcal{F}(S))$. The dimension of S therefore increases by at most a factor of four (with equality when $\{M_i, M_i^\dagger, XM_iX, XM_i^\dagger X\}$ are all linearly independent). $\square$

The other ingredient, namely a family of strongly unextendible subspaces, is provided by the well-known *unextendible product bases.*

Definition 21 *An* unextendible product basis *(UPB) is a set of product states $\{|\psi_i\rangle_{AB}\}$ (not necessarily orthogonal) in a bipartite space $\mathcal{H}_A \otimes \mathcal{H}_B$ such that $(\mathrm{span}\{|\psi_i\rangle\})^\perp$ contains no product states. The* dimension *of a UPB is the number of product states in the set.*

Clearly, a UPB spans a 1-unextendible subspace. That this subspace is in fact strongly unextendible is shown by the following lemma.

Lemma 22 *If $\{|\psi_i^1\rangle_{A_1B_1}\}$ and $\{|\psi_i^2\rangle_{A_2B_2}\}$ are unextendible product bases in $\mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}$ and $\mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2}$ respectively, then $\{|\psi_i^1\rangle\,|\psi_j^2\rangle\}_{i,j}$ is an unextendible product basis in $\mathcal{H}_{A_1A_2} \otimes \mathcal{H}_{B_1B_2}$.*

Proof If $\{|\psi_i^1\rangle_{A_1B_1}\}$ and $\{|\psi_i^2\rangle_{A_2B_2}\}$ are both orthogonal unextendible product bases, this case was proved in Ref. [22]. For non-orthogonal unextendible

product bases, let $|\psi_i^1\rangle_{A_1B_1} = |\alpha_i^1\rangle_{A_1}|\beta_i^1\rangle_{B_1}$ for $1 \le i \le k_1$ and $|\psi_j^2\rangle_{A_2B_2} = |\alpha_j^2\rangle_{A_2}|\beta_j^2\rangle_{B_2}$ for $1 \le j \le k_2$.

Assume for contradiction that $\{|\psi_i^1\rangle|\psi_j^2\rangle\}_{i,j}$ is extendible in $\mathcal{H}_{A_1A_2} \otimes \mathcal{H}_{B_1B_2}$ which means there exists a product state $|x\rangle_{A_1A_2}|y\rangle_{B_1B_2}$ in $\mathcal{H}_{A_1A_2} \otimes \mathcal{H}_{B_1B_2}$ which is orthogonal to any $|\psi_i^1\rangle_{A_1B_1}|\psi_j^2\rangle_{A_2B_2}$. We then have

$$\forall\ 1 \le i \le k_1 \text{ and } 1 \le j \le k_2 :\ \langle\alpha_i^1, \alpha_j^2|x\rangle\,\langle\beta_i^1, \beta_j^2|y\rangle = 0. \tag{61}$$

For an $m \times n$ matrix A, $\mathrm{vec}(A)$ is an mn–element column vector whose first m elements are the first column of A, the next m elements are the second column of A, and so on. Thus "vec" converts the matrix into a vector. In "vec" notation, we have $\mathrm{vec}(ABC) = (C^T \otimes A)\,\mathrm{vec}(B)$. Applying this, we obtain

$$0 = \langle\alpha_i^1, \alpha_j^2|x\rangle_{A_1A_2}\,\langle\bar{y}|\bar{\beta}_i^1, \bar{\beta}_j^2\rangle_{B_1B_2} \tag{62a}$$

$$= \langle\alpha_i^1|_{A_1}\left(\mathbb{1}_{A_1} \otimes \langle\alpha_j^2|_{A_2}\right)\left(|x\rangle_{A_1A_2}\langle\bar{y}|_{B_1B_2}\right)\left(\mathbb{1}_{B_1} \otimes |\bar{\beta}_j^2\rangle_{B_2}\right)|\bar{\beta}_i^1\rangle_{B_1} \tag{62b}$$

$$= \left(|\bar{\beta}_i^1\rangle_{B_1}^T \otimes \langle\alpha_i^1|_{A_1}\right)\mathrm{vec}\Big(\left(\mathbb{1}_{A_1} \otimes \langle\alpha_j^2|_{A_2}\right)\left(|x\rangle_{A_1A_2}\langle\bar{y}|_{B_1B_2}\right)\left(\mathbb{1}_{B_1} \otimes |\bar{\beta}_j^2\rangle_{B_2}\right)\Big) \tag{62c}$$

$$= \langle\beta_i^1|_{B_1}\langle\alpha_i^1|_{A_1}\Big((\mathbb{1}_{B_1} \otimes |\bar{\beta}_j^2\rangle_{B_2})^T \otimes (\mathbb{1}_{A_1} \otimes \langle\alpha_j^2|_{A_2})\Big)\,\mathrm{vec}\Big(|x\rangle_{A_1A_2}\langle\bar{y}|_{B_1B_2}\Big) \tag{62d}$$

$$= \langle\beta_i^1|_{B_1}\langle\alpha_i^1|_{A_1}\Big(\mathbb{1}_{B_1} \otimes \langle\beta_j^2|_{B_2} \otimes \mathbb{1}_{A_1} \otimes \langle\alpha_j^2|_{A_2}\Big)\Big(\langle\bar{y}|_{B_1B_2}^T \otimes |x\rangle_{A_1A_2}\Big)\,\mathrm{vec}(\mathbb{1}) \tag{62e}$$

$$= \langle\beta_i^1|_{B_1}\langle\alpha_i^1|_{A_1}\Big[\Big(\mathbb{1}_{B_1} \otimes \langle\beta_j^2|_{B_2}\Big)|y\rangle_{B_1B_2} \otimes \Big(\mathbb{1}_{A_1} \otimes \langle\alpha_j^2|_{A_2}\Big)|x\rangle_{A_1A_2}\Big]. \tag{62f}$$

For any fixed j, the term in square brackets is either the zero vector, or a product state in $\mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}$ which is orthogonal to any $|\psi_i^1\rangle_{A_1B_1} = |\alpha_i^1\rangle_{A_1}|\beta_i^1\rangle_{B_1}$. But $\{|\psi_i^1\rangle_{A_1B_1}\}$ is an unextendible product basis, so if it is non-zero for some j then we have a contradiction.

Otherwise, $\left(\mathbb{1}_{B_1} \otimes \langle\beta_j^2|_{B_2}\right)|y\rangle_{B_1B_2} \otimes \left(\mathbb{1}_{A_1} \otimes \langle\alpha_j^2|_{A_2}\right)|x\rangle_{A_1A_2} = 0$ for any j. Let $|\gamma\rangle_{B_1}$ and $|\delta\rangle_{A_1}$ be two vectors such that $\left(\langle\gamma|_{B_1} \otimes \mathbb{1}_{B_2}\right)|y\rangle_{B_1B_2} \neq 0$ and $\left(\langle\delta|_{A_1} \otimes \mathbb{1}_{A_2}\right)|x\rangle_{A_1A_2} \neq 0$. Then we have

$$\langle\beta_j^2|_{B_2}\langle\alpha_j^2|_{A_2}\Big[\left(\langle\gamma|_{B_1} \otimes \mathbb{1}_{B_2}\right)|y\rangle_{B_1B_2} \otimes \left(\langle\delta|_{A_1} \otimes \mathbb{1}_{A_2}\right)|x\rangle_{A_1A_2}\Big] = 0 \tag{63}$$

for any j. Here, the term in square brackets is a nonzero product state in $\mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2}$ which is orthogonal to any $|\psi_j^2\rangle_{A_2B_2} = |\alpha_j^2\rangle_{A_2}|\beta_j^2\rangle_{B_2}$. But $\{|\psi_j^2\rangle_{A_2B_2}\}$ is also an unextendible product basis, which gives a contradiction as before. □

Lemma 22 says that tensor products of unextendible product bases are unextendible, which in particular implies that all tensor powers of an unextendible product basis are unextendible, i.e. unextendible product bases span strongly unextendible subspaces. The following lemma giving the minimal dimension of a UPB was proven in Ref. [23]:

Lemma 23 *There exists a UPB of dimension m in $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ for any $d_A + d_B - 1 \le m \le d_A d_B$.*

We are now in a position to prove the existence of strongly unextendible subspaces in F_d (i.e. strongly unextendible subspaces obeying the symmetry constraints of Eqs. (41c) and (41d) from Theorem 13), for sufficiently large dimension. (It turns out that 16 is "sufficiently large" enough.)

Lemma 24 *For $U = \mathbb{1}$, $V = X$, there exist strongly unextendible subspaces $S \in F_d(\mathbb{C}, d_A)$ of dimension d for any $4(2d_A - 1) \leq d \leq d_A^2$.*

Proof Let S be a subspace spanned by a UPB with the minimal dimension $m = 2d_A - 1$. Lemma 23 tells us that S is strongly unextendible. By Lemma 20, its symmetrisation $\mathcal{F}(S)$ has dimension at most $4m = 4(2d_A - 1)$. Also, since symmetrising can never shrink the subspace, we have $\mathcal{F}(S)^\perp \subseteq S^\perp$ so $\mathcal{F}(S)$ is also strongly unextendible.

Thus $\mathcal{F}(S)$ is a strongly unextendible subspace of dimension at most $4(2d_A - 1)$. The lemma follows from the fact that any extension $S' \supseteq S$ is strongly unextendible if S is. □

Combining Theorem 19 and Lemma 24, we have shown that:

Corollary 25 *For $d \geq 4(2d_A - 1)$ and $U = \mathbb{1}$, $V = X$, the set of strongly unextendible subspaces $U_d(\mathcal{H}_A, \mathcal{H}_{A'}) \cap F_d(\mathbb{C}, d_A)$ is full measure in $F_d(\mathbb{C}, d_A)$.*

This leads to the main theorem of this section.

Theorem 26 *For $d_A \geq 16$, $U = \mathbb{1}$, $V = X$, and for a subspace $S \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_A}$ of dimension $4(2d_A - 1) \leq d \leq d_A^2 - 4(2d_A - 1)$ chosen uniformly at random subject to the symmetry constraints $\mathbb{F}(S) = S$ and $\mathbb{F}(U \otimes V \cdot S) = U \otimes V \cdot S$, both S and $S^\perp$ will almost-surely be strongly unextendible.*

Proof Corollary 25 implies that S chosen in this way will almost-surely be strongly unextendible. But $S^\perp$ is then a random subspace subject to the same symmetry constraints, with dimension $4(2d_A - 1) \leq d^\perp = d_A^2 - d \leq d_A^2 - 4(2d_A - 1)$. Thus Corollary 25 implies that $S^\perp$ will be almost-surely strongly unextendible. For there to exist a suitable d, we require $4(2d_A - 1) \leq d_A^2 - 4(2d_A - 1)$, or $d_A \geq 16$. □

5.3 Positive-semidefinite conjugate-symmetric subspaces

Theorem 26 shows that a random subspace satisfying the symmetry constraints of Eqs. (41c) and (41d) from Theorem 13 will in fact also almost-surely satisfy the strong unextendibility requirements of Eqs. (41a) and (41b). It remains to show that the positive-semidefiniteness requirements of Eqs. (41e) and (41f) can also be satisfied simultaneously.

Theorem 27 *If d_A is even, $\lfloor d/2 \rfloor \leq d_A^2/2 - 1$ and $U = \mathbb{1}$, $V = X$, then the set*

$$P_d(d_A) = \{S \in F_d(\mathbb{C}, d_A) \,|\, S \text{ and } U \otimes V \cdot S^\perp \text{ positive-semidefinite}\} \qquad (64)$$

has non-zero measure in $F_d(\mathbb{C}, d_A)$.

Before proving Theorem 27, we will state a lemma about the structure of $F_d(\mathbb{R}, d_A)$ when d_A is even.

Lemma 28 *If d_A is even and $U = \mathbb{1}$, $V = X$, then*

$$F_d(\mathbb{R}, d_A) \cong \bigoplus_{k=0}^{d} \mathrm{Gr}_k(\mathbb{R}^{d_A^2/2}) \times \mathrm{Gr}_{d-k}(\mathbb{R}^{d_A^2/2}). \tag{65}$$

In other words an element of $F_d(\mathbb{R}, d_A)$ can be uniquely identified by specifying an integer $0 \leq k \leq d$ and elements of $\mathrm{Gr}_k(\mathbb{R}^{d_A^2/2})$ and $\mathrm{Gr}_{d-k}(\mathbb{R}^{d_A^2/2})$.

Proof (of Lemma 28) Elements of $F_d(\mathbb{R}, d_A)$ are $2d$-dimensional real subspaces of $\mathbb{R}^2 \otimes \mathbb{R}^{d_A} \otimes \mathbb{R}^{d_A}$. As such, they can be expressed as rank-$2d$ projectors. The constraints in Eq. (52) defining $F_d(\mathbb{R}, d_A)$ can be expressed as symmetries of these projectors. In particular, $\Pi \in F_d(\mathbb{R}, d_A)$ if and only if Π is a rank-$2d$ projector satisfying $i\,\Pi\, i^T = \Pi$, $\mathbb{F}\,\Pi\,\mathbb{F}^T = \Pi$ and $(X \otimes X)\Pi(X \otimes X) = \Pi$.

Initially we will consider the i and $\mathbb{F}$ symmetries. Let $\mathbb{F}_\pm$ denote the ± 1 eigenspaces of $\mathbb{F}$. Since Π commutes with $\mathbb{F}$, it must be the sum of a projector onto a subspace of $\mathbb{F}_+$ and a projector onto a subspace of $\mathbb{F}_-$. In other words, $\Pi = \Pi_+ + \Pi_-$ where $\Pi_\pm\,\mathbb{F} = \mathbb{F}\,\Pi_\pm = \pm\Pi_\pm$. Since i and $\mathbb{F}$ anticommute, i must map $\mathbb{F}_\pm$ to $\mathbb{F}_\mp$. Thus $i\,\Pi_+ i^T$ is a projector onto $\mathbb{F}_-$ and $i\,\Pi_- i^T$ is a projector onto $\mathbb{F}_+$. Combined with the fact that $i\,\Pi\, i^T = \Pi$ we obtain that $i\,\Pi_\pm i^T = \Pi_\mp$. We can thus assume that $\Pi = \Pi_+ + i\,\Pi_+ i^T$ where Π_+ is a projector onto $\mathbb{F}_+$. Since Π has rank $2d$, Π_+ must have rank d.

Since $X \otimes X$ commutes with $\mathbb{F}$ and Π, we have that Π_+ must also commute with $X \otimes X$. This means we can write Π_+ as $\Pi_{++} + \Pi_{+-}$, where Π_{++} is a projector onto a subspace of the $+1$ eigenspace of $X \otimes X$ and Π_{+-} projects onto a subspace of the -1 eigenspace of $X \otimes X$.

Working backwards we can see that if Π_{++}, Π_{+-} are arbitrary projectors with the appropriate supports and with ranks summing to d, then $\Pi = (\Pi_{++} + \Pi_{+-}) + i(\Pi_{++} + \Pi_{+-})i^T$ projects onto a subspace in $F_d(\mathbb{R}, d_A)$. If Π_{++} has rank k then our choice of Π is equivalent to choosing an element of $\mathrm{Gr}_k(\mathbb{R}^{d_A^2/2}) \times \mathrm{Gr}_{d-k}(\mathbb{R}^{d_A^2/2})$. $\square$

Proof (of Theorem 27) To understand what it means to have non-zero measure in $F_d(\mathbb{C}, d_A)$, we use Lemma 28 and the fact that $\dim \mathrm{Gr}_k(\mathbb{R}^{d_A^2/2}) = (d_A^2/2 - k)k$. Thus

$$\begin{aligned}\dim\left(\mathrm{Gr}_k(\mathbb{R}^{d_A^2/2}) \times \mathrm{Gr}_{d-k}(\mathbb{R}^{d_A^2/2})\right) &= \left(\frac{d_A^2}{2} - k\right) k \left(\frac{d_A^2}{2} - d + k\right)(d-k) \\ &= k(d-k)\left(\frac{d_A^2}{2}\left(\frac{d_A^2}{2} - d\right) - k(d-k)\right),\end{aligned}$$

which takes its maximum value at $k = d/2$ (for d even) or $k = (d \pm 1)/2$ (for d odd). This means that all but a measure-zero subset of $F_d(\mathbb{C}, d_A)$ is contained in these values of k. Indeed, if k is even then the component of $F_d(\mathbb{C}, d_A)$ corresponding to $\mathrm{Gr}_{d/2}(\mathbb{R}^{d_A^2/2}) \times \mathrm{Gr}_{d/2}(\mathbb{R}^{d_A^2/2})$ has measure one in $F_d(\mathbb{C}, d_A)$. If k is odd then the components corresponding to $\mathrm{Gr}_{(d+1)/2}(\mathbb{R}^{d_A^2/2}) \times \mathrm{Gr}_{(d-1)/2}(\mathbb{R}^{d_A^2/2})$ and $\mathrm{Gr}_{(d-1)/2}(\mathbb{R}^{d_A^2/2}) \times \mathrm{Gr}_{(d+1)/2}(\mathbb{R}^{d_A^2/2})$ each have measure $1/2$. For the rest of the proof we will take k to be $d/2$ for d even or $(d-1)/2$ for d odd. Let $\hat{F}_d(\mathbb{C}, d_A)$ denote the part of $\mathbb{F}(\mathbb{C}, d_A)$ corresponding to $\mathrm{Gr}_{d/2}(\mathbb{R}^{d_A^2/2}) \times \mathrm{Gr}_{d/2}(\mathbb{R}^{d_A^2/2})$ if d is even or $\mathrm{Gr}_{(d+1)/2}(\mathbb{R}^{d_A^2/2}) \times \mathrm{Gr}_{(d-1)/2}(\mathbb{R}^{d_A^2/2})$ if d is odd.

In either case, it suffices to show that $P_d(d_A) \cap \hat{F}_d(\mathbb{C}, d_A)$ has positive measure in $\hat{F}_d(\mathbb{C}, d_A)$. To do so, we first construct a positive-*definite* subspace $S \in \hat{F}_d(\mathbb{C}, d_A)$, meaning a subspace S with a positive-definite basis. We would also like $(\mathbb{1} \otimes X) \cdot S^\perp$ to be positive-definite. This will guarantee that every $S' \in \hat{F}_d(\mathbb{C}, d_A)$ that is sufficiently close to S will belong to $P_d(d_A) \cap \hat{F}_d(\mathbb{C}, d_A)$, implying that this set has non-zero measure and proving the theorem.

It remains only to construct the desired S. As we have observed in Proposition 8, for S to be positive definite, it is sufficient for $\mathbb{M}(S)$ to contain a single positive-definite element. In particular, we will choose S to contain $|\omega\rangle = \sum_{i=1}^{d_A} |i, i\rangle$. We will also require that S be orthogonal to $(\mathbb{1} \otimes X)|\omega\rangle$ so that $(\mathbb{1} \otimes X)S^\perp$ also contains $|\omega\rangle$ and is positive definite. Note that this only works if d_A is even, otherwise $|\omega\rangle$ and $(\mathbb{1} \otimes X)|\omega\rangle$ are not orthogonal.

Both $|\omega\rangle$ and $(\mathbb{1} \otimes X)|\omega\rangle$ belong to the $+1$ eigenspace of $X \otimes X$. Thus to choose S we need only choose an additional $k - 1$ dimensions for Π_{++} (from a space of dimension $d_A^2/2 - 2$) as well as an arbitrary rank-$(d - k)$ projector Π_{+-} whose support is contained within the -1 eigenspace of $X \otimes X$ (with dimension $d_A^2/2$). This is possible as long as $k \leq d_A^2/2 - 1$ and $d - k \leq d_A^2/2$. Substituting our choice of k, we find that it suffices to take $\lfloor d/2 \rfloor \leq d_A^2/2 - 1$. □

5.4 Superactivation of the zero-error capacity

Theorem 26 shows that, for suitable dimensions, a subspace chosen at random subject to the symmetry constraints of Eqs. (41c) and (41d) from Theorem 13 will, with probability 1, satisfy the strong unextendibility conditions of Eqs. (41a) and (41b). But Theorem 27 shows that there is a non-zero probability that such a random subspace will satisfy the positivity conditions of Eqs. (41e) and (41f). Therefore, there must exist at least one subspace S satisfying all the conditions of Theorem 13. Finally, we use Proposition 9 to translate S and $U \otimes V \cdot S^\perp$ into channels and complete the proof of superactivation of the zero-error classical capacity of quantum channels, as stated in Theorem 1 (Section 1), the main result of this paper.

"Suitable dimensions" are any set of channel input and output dimensions d_A and d_B, together with a number of Kraus operators d_E, that simultaneously satisfy all the dimension requirements of Theorems 26 and 27. Note that, from Proposition 9, d_E is given by the dimension of the subspace. In fact, the upper bound on the subspace dimension from Theorem 27 is always satisfied if that of Theorem 26 is. Also, the requirement from Theorem 27 that d_A be even merely implies that the input dimension to the channel itself must be *larger* than an even number, since we can always embed a channel in a higher-dimensional input space. So the minimal dimension requirements reduce to those stated in Theorem 1.

6 Conclusions

Smith and Yard's result [10] showed that the capacity of quantum channels to communicate quantum information behaves in the most surprising way conceivable: two channels with zero capacity for transmitting quantum information can nonetheless transmit quantum information when used together (*superactivation*). On the other hand, although it is very likely non-additive [7], the usual

classical Shannon capacity of quantum channels cannot behave in this extreme way.

However, in this work we have shown that the capacity of a quantum channel for transmitting classical information *perfectly*, the zero-error classical capacity, exhibits the same surprising phenomenon as the quantum capacity: two channels with zero capacity for perfect transmission of classical information can nonetheless transmit classical information perfectly when used together. This is, to our knowledge, the first ever proven superactivation of a *classical* capacity of a standard quantum channel. (Note that although the zero-error capacity of classical channels is non-additive, superactivation is impossible classically.) It shows that this remarkable feature of quantum channels, to allow communication when seemingly none should be possible, is not restricted to quantum information but also occurs for classical information.

How is this surprising behaviour possible? In the case of the quantum capacity, superactivation is achieved *without* the inputs to the two channels needing to be entangled, and the intuition behind the superactivation has more to do with local indistinguishability of orthogonal quantum states [24]. But entanglement *is* responsible for the superactivation of the zero-error capacity, just as it is necessary if the standard classical Shannon capacity of quantum channels is to be non-additive. So the fact that superactivation of the zero-error classical capacity occurs for quantum but not for classical channels can be attributed to the use of entangled inputs, which have no classical analogue.

The results of Section 5 also resolve a number of other questions. For one, they imply that the zero-error capacity of the multi-sender/multi-receiver quantum channels of Duan and Shi [18] can also be superactivated (extending their one-shot result to the full asymptotic capacity). They also imply that even the regularised version of the minimum output Rényi 0-entropy investigated in Ref. [9] is non-additive. In and of itself, this is perhaps just a mathematical curiosity. But the same result for the minimum output *von Neumann* entropy (the Rényi 1-entropy) would imply that the classical Shannon capacity of quantum channels really is non-additive (i.e. that the capacity of two channels used together could be greater than the sum of their individual capacities).

We close with an open question. Do there exist channels $\mathcal{E}_1, \mathcal{E}_2$ with no zero-error classical capacity individually, but such that $\mathcal{E}_1 \otimes \mathcal{E}_2$ has a positive zero-error *quantum* capacity?

Note Added: Simultaneously with our results, Duan [25] extended his previous work to prove that the one-shot zero-error capacity can also be superactivated in the case of single-input, single-output channels. He also proves that the zero-error capacity is strongly non-additive in the following sense: a quantum channel that has no zero-error classical capacity can boost the zero-error capacity of a second channel, which however does have some zero-error capacity on its own. Whilst non-additivity of the zero-error capacity occurs even for classical channels, this stronger form of non-additivity is impossible classically. Both these results are implied by our stronger result, which proves full superactivation in the standard sense (i.e. *both* channels have zero capacity) for the *asymptotic* capacity (i.e. even infinitely many copies of the individual channels have zero capacity). However, interestingly Duan's techniques are different to ours, and also prove a similar non-additivity of the *quantum* zero error capacity, which our paper does not address.

7 Acknowledgements

We would like to thank Andreas Winter for very useful discussions about this work, and for pointing out the implications of our results to non-additivity of regularised Rényi entropies. We also thank Runyao Duan for kindly sending us a version of his latest results prior to publication. TSC is supported by a Leverhulme early-career fellowship. JC is supported by The China Scholarship Council. AWH and TSC acknowledge support through the integrated EC project "QAP" (contract no. IST-2005-15848), and AWH was also funded by the U.K. EPSRC grant "QIP IRC."

References

[1] A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Trans. Inform. Theory*, 44:269–273, 1998. (arXiv:quant-ph/9611023).

[2] B. Schumacher and M. D. Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A*, 56:131, 1997.

[3] Igor Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inform. Theory*, 51:44, 2005. (arXiv:quant-ph/0304127).

[4] P. W. Shor. The quantum channel capacity and coherent information. MSRI seminar, November 2002.

[5] S. Lloyd. Capacity of the noisy quantum channel. *Phys. Rev. A*, 55:1613, 1996.

[6] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin. Quantum channel capacity of very noisy channels. *Phys. Rev. A*, 57:830, 1998. (arXiv:quant-ph/9706061).

[7] M. B. Hastings. A counterexample to additivity of minimum output entropy. *Nature Physics*, 5, 2009. (arXiv:0809.3972 [quant-ph]).

[8] A. J. Winter and P. Hayden. Counterexamples to the maximal p-norm multiplicativity conjecture for all $p > 1$. *Commun. Math. Phys.*, 284(1):263, 2008. (arXiv:0807.4753 [quant-ph]).

[9] T. Cubitt, A. W. Harrow, D. Leung, A. Montanaro, and A. Winter. Counterexamples to additivity of minimum output p-rényi entropy for p close to 0. *Commun. Math. Phys.*, 284:281, 2008. (arXiv:0712.3628 [quant-ph]).

[10] G.B. Smith and J. Yard. Quantum communication with zero-capacity channels. *Science*, 321:1812, 2008. (arXiv:0807.4935 [quant-ph]).

[11] P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Superactivation of bound entanglement. arXiv:quant-ph/0005117, 2000.

[12] K. Li, A.J. Winter, X.B. Zou, and G.C. Guo. Nonadditivity of the private classical capacity of a quantum channel. arXiv:0903.4308 [quant-ph], 2009.

[13] G.B. Smith and J.A. Smolin. Extensive nonadditivity of privacy. arXiv:0904.4050 [quant-ph], 2009.

[14] C. E. Shannon. The zero-error capacity of a noisy channel. *IRE Trans. Inform. Theory*, IT-2:8, 1956.

[15] J. Körner and A. Orlitsky. Zero-error information theory. *IEEE Trans. Inform. Theory*, 44(6):2207, 1998.

[16] R. A. C. Medeiros and F. M. de Assis. Quantum zero-error capacity. *Int. J. Quant. Inf.*, 3:135, 2005.

[17] S. Beigi and P. W. Shor. On the complexity of computing zero-error and holevo capacity of quantum channels. arXiv:0709.2090 [quant-ph], 2007.

[18] R. Duan and Y. Shi. Entanglement between two uses of a noisy multipartite quantum channel enables perfect transmission of classical information. *Phys. Rev. Lett.*, 2008. (arXiv:0712.3700 [quant-ph]).

[19] Runyao Duan, Jianxin Chen, and Yu Xin. Unambiguous and zero-error classical capacity of noisy quantum channels. (Manuscript in preparation).

[20] T. Cubitt, A. Montanaro, and A. Winter. On the dimension of subspaces with bounded schmidt rank. *J. Math. Phys.*, 49:022107, 2008. (arXiv:0706.0705 [quant-ph]).

[21] Joe Harris. *Algebraic Geometry*. Springer-Verlag, 1992.

[22] D. DiVincenzo, T. Mor, P. W. Shor, J.A. Smolin, and B.M. Terhal. Unextendible product bases, uncompletable product bases and bound entanglement. *Commun. Math. Phys.*, 238(3):379, 2003.

[23] R. Bhat. A completely entangled subspace of maximal dimension. *Int. J. Quant. Inf.*, 4(2):325, 2006.

[24] Jonathan Oppenheim. For quantum information, two wrongs can make a right. *Science Perspectives*, 321(5897):1783, 2008.

[25] R. Duan. Superactivation of zero-error capacity of noisy quantum channels. arXiv:0906.2527 [quant-ph], 2009.